

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY



(Chapter II of the Patent Cooperation Treaty)

(PCT Article 36 and Rule 70)

REC'D 25 AUG 2005

WIPO

PCT

Applicant's or agent's file reference PCT-170		FOR FURTHER ACTION		See Form PCT/PEA/416
International application No. PCT/EP2004/051217		International filing date (day/month/year) 23.06.2004	Priority date (day/month/year) 26.06.2003	
International Patent Classification (IPC) or national classification and IPC H04L29/06, H04L12/46				
Applicant TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) et al.				
<p>1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.</p> <p>2. This REPORT consists of a total of 5 sheets, including this cover sheet.</p> <p>3. This report is also accompanied by ANNEXES, comprising:</p> <p>a. <input checked="" type="checkbox"/> sent to the applicant and to the International Bureau) a total of 7 sheets, as follows:</p> <p><input checked="" type="checkbox"/> sheets of the description, claims and/or drawings which have been amended and are the basis of this report and/or sheets containing rectifications authorized by this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions).</p> <p><input type="checkbox"/> sheets which supersede earlier sheets, but which this Authority considers contain an amendment that goes beyond the disclosure in the international application as filed, as indicated in item 4 of Box No. I and the Supplemental Box.</p> <p>b. <input type="checkbox"/> (sent to the International Bureau only) a total of (indicate type and number of electronic carrier(s)) , containing a sequence listing and/or tables related thereto, in computer readable form only, as indicated in the Supplemental Box Relating to Sequence Listing (see Section 802 of the Administrative Instructions).</p>				
<p>4. This report contains indications relating to the following items:</p> <p><input checked="" type="checkbox"/> Box No. I Basis of the opinion</p> <p><input type="checkbox"/> Box No. II Priority</p> <p><input type="checkbox"/> Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability</p> <p><input type="checkbox"/> Box No. IV Lack of unity of invention</p> <p><input checked="" type="checkbox"/> Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement</p> <p><input type="checkbox"/> Box No. VI Certain documents cited</p> <p><input type="checkbox"/> Box No. VII Certain defects in the international application</p> <p><input type="checkbox"/> Box No. VIII Certain observations on the international application</p>				
Date of submission of the demand 20.04.2005		Date of completion of this report 26.08.2005		
Name and mailing address of the International preliminary examining authority:		Authorized Officer		
 <p>European Patent Office - P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Tx: 31 651 epo nl Fax: +31 70 340 - 3016</p>		<p>Veen, G</p> <p>Telephone No. +31 70 340-3811</p> 		

**INTERNATIONAL PRELIMINARY REPORT
ON PATENTABILITY**

International application No.
PCT/EP2004/051217

Box No. I Basis of the report

1. With regard to the **language**, this report is based on the international application in the language in which it was filed, unless otherwise indicated under this item.

☐ This report is based on translations from the original language into the following language , which is the language of a translation furnished for the purposes of:

- ☐ international search (under Rules 12.3 and 23.1(b))
- ☐ publication of the international application (under Rule 12.4)
- ☐ international preliminary examination (under Rules 55.2 and/or 55.3)

2. With regard to the **elements*** of the international application, this report is based on *(replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report)*:

Description, Pages

1-20 as originally filed

Claims, Numbers

1-23 received on 08.08.2005 with letter of 08.08.2005

Drawings, Sheets

1/6-6/6 as originally filed

☐ a sequence listing and/or any related table(s) - see Supplemental Box Relating to Sequence Listing

3. ☐ The amendments have resulted in the cancellation of:

- ☐ the description, pages
- ☐ the claims, Nos.
- ☐ the drawings, sheets/figs
- ☐ the sequence listing (*specify*):
- ☐ any table(s) related to sequence listing (*specify*):

4. ☐ This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

- ☐ the description, pages
- ☐ the claims, Nos.
- ☐ the drawings, sheets/figs
- ☐ the sequence listing (*specify*):
- ☐ any table(s) related to sequence listing (*specify*):

* If item 4 applies, some or all of these sheets may be marked "superseded."

**INTERNATIONAL PRELIMINARY REPORT
ON PATENTABILITY**

International application No.
PCT/EP2004/051217

Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes: Claims	
	No: Claims	1-23
Inventive step (IS)	Yes: Claims	
	No: Claims	1-23
Industrial applicability (IA)	Yes: Claims	
	No: Claims	1-23

2. Citations and explanations (Rule 70.7):

see separate sheet

Re Item V.

- 1 The following documents are referred to in this communication:
D1 : US 6 571 289 B1 (MONTENEGRO GABRIEL E) 27 May 2003 (2003-05-27)
D2 : US 6 253 327 B1 (LOU SHUXIAN ET AL) 26 June 2001 (2001-06-26)
- 2 The present application does not meet the criteria of Article 33(1) PCT, because the subject matter of claims 1-23 does not involve an inventive step in the sense of Article 33(3)PCT.
 - 2.1 **INDEPENDENT CLAIM 1**
In the words of claim 1, D1 discloses (references taken from D1):

"An apparatus arranged for receiving a ~~Single Sign-On~~ service request in a telecommunication service network from a user via an access network (column 1, line 63) unable to provide data origin authentication (c1l64; c3l31-33), the user having received access credentials as a result of being authenticated by a core network (c3l41-43), the apparatus comprising:

 - means for receiving the access credentials from the user through the access network (c3l15-16; c3l20; c3l35; c3l41-43; c3l50-54);
 - means for checking validity of the access credentials received from the user (c3l64-66);
 - means for establishing a valid session with the user upon successful validity check of the access credentials (c3l66-c4l3);
 - means for assigning an internal IP address to identify the user in the service network (c4l15-19); and
 - means for linking session data, access credentials and assigned internal IP address for the user (c3l66-c4l53); and

characterised in that it includes:

 - means for establishing a secure tunnel with the user when receiving the access credentials through the access network (c3l66-c4l1) by using an outer IP address assigned to the user by the access network for addressing the user (c4l25-27; c4l33-36), and by using the internal IP address assigned to identify the user in the service

network as an inner IP address in the tunnelled traffic."

Claim 1 differs from D1 in that it employs a single-sign-on mechanism. The problem to be solved by the present invention may therefore be regarded as "How to allow a user to access multiple services, without having to successfully complete each of their respective authentication procedures first?"

D2 discloses a single-step logon process which grants a subscriber access to one or more public domains and one or more private domains, without requiring the subscriber to launch a separate logon procedure for each of them, thereby solving said problem (see D2, c4130-47).

As both documents are in the same technical field (authentication in computer networks) the person skilled in the art, faced with the above stated problem, and the prior art as represented by D1 and D2, would apply the invention of D2 to the system of D1 to arrive at the claimed subject-matter. Thus claim 1 does not involve an inventive step and is therefore obvious.

2.2 INDEPENDENT CLAIMS 14 AND 18

The same argumentation applies to independent claims 14 and 18 which define a user equipment and a method corresponding to the apparatus of claim 1. Therefore these claims also lack an inventive step in the sense of Art. 33(3) PCT.

2.3 CLAIMS 2-13, 15-17 AND 19-23

Dependent claims 2-13, 15-17 and 19-23 do not contain any features which, in combination with the features of any claim to which they refer, meet the requirements of the PCT in respect of novelty and/or inventive step (Article 33(2) and (3) PCT).

REPLACEMENT SHEET

21

EPO - DG 1

08.08.2005

CLAIMS

(82)

1. An apparatus (N-41, N-42) arranged for receiving a Single Sign-On service request in a telecommunication service network (N-40) from a user (N-10) via an access network (N-20) unable to provide data origin authentication, the user (N-10) having received (S-23) access credentials (Digital Certificate) as a result of being authenticated by a core network (N-30), the apparatus comprising:

- means for receiving (S-24) the access credentials from the user (N-10) through the access network (N-20);

- means for checking (N-41; S-25, N-31) validity of the access credentials received from the user (N-10);

- means for establishing a valid session with the user (N-10) upon successful validity check of the access credentials;

- means for assigning an internal IP address to identify the user in the service network (N-40); and

- means for linking (N-41, S-26, N-42) session data, access credentials and assigned internal IP address for the user (N-10);

and characterised in that it includes:

- means for establishing a secure tunnel (S-24) with the user (N-10) when receiving the access credentials through the access network (N-20) by using an outer IP address assigned to the user by the access network for addressing the user, and by using the internal IP address assigned to identify the user in the service network (N-40) as an inner IP address in the tunnelled traffic.

REPLACEMENT SHEET

22

2. The apparatus of claim 1, further comprising means for generating service credentials (N-41, S-26, N-42) for authorizing the user to access a service in the service network (N-40).
- 5 3. The apparatus of claim 2, wherein the service credentials are generated (N-41, S-26, N-42) on a per service basis for the user upon service request.
- 10 4. The apparatus of claim 1, further comprising means for communicating (S-25) with an Authentication Server (N-31) of the home network (N-30) in order to check the validity of the access credentials received from the user (N-10), when said access credentials are not signed by a recognised authentication entity (N-31).
- 15 5. The apparatus of claim 1, wherein the means for establishing the secure tunnel (S-24) with the user (N-10) are included in a first device named Secure Service Entry Point (N-41), and the means for linking session data, access credentials and assigned internal IP address for the user (N-10) are included in a second device named
- 20 Single Sign-On server (N-42).
6. The apparatus of claim 5, further comprising means for communicating (S-26) the Secure Service Entry Point (N-41) with the Single Sign On Server (N-42).
- 25 7. The apparatus of claim 1, further comprising means for an additional co-ordination (S-25) between the apparatus (N-41; N-42) and an Identity Provider (N-31) in charge of said user in a home network (N-30) when said home network is different than the service network (N-40) which the apparatus is the entry point for.
- 30 8. The apparatus of claim 1 for use when the user (N-10) is accessing a local HTTP service (N-44), or an external service (N-51) in a network (N-50) different than the

AMENDED SHEET

REPLACEMENT SHEET

23

currently accessed service network (N-40), the apparatus having means for checking (N-41, S-30, N-43, S-28, N-42) whether the user had been previously authenticated or not.

- 5 9. The apparatus of claim 8, having means (S-30, S-28) for communicating with an intermediate entity (N-43) arranged to intercept the user's access (S-29) to the HTTP local service (N-44), or to the external service (N-51) in an external network (N-50).
- 10 10. The apparatus of claim 9, wherein the intermediate entity (N-43) is an HTTP-proxy.
11. The apparatus of claim 9, wherein the intermediate entity (N-43) is a firewall.
- 15 12. The apparatus of claim 1 for use when the user (N-10) is accessing a non-HTTP local service (N-45), having means for checking (N-41, S-31, N-45, S-32, N-42) whether the user had been previously authenticated or not.
- 20 13. The apparatus of claim 1, wherein the means for receiving access credentials comprises means for checking whether a digital certificate issued by the core network is present to indicate a successful authentication of the user.
- 25 14. A user equipment (N-10; N-11) arranged to carry out an authentication procedure with a core network (N-30), and arranged to access a telecommunication service network (N-40) via an access network (N-20) unable to provide data origin authentication, the user equipment (N-10; N-11) comprising:
- 30 - means for obtaining (S-23) access credentials as a result of being authenticated by the core network (N-30);

REPLACEMENT SHEET

24

- means for sending (S-24) the access credentials towards the service network (N-40) when accessing through the access network (N-20)

and characterised in that it includes:

- 5 - means for establishing a secure tunnel (S-24) with the service network (N-40) through the access network (N-20), the secure tunnel making use of an outer IP address assigned to the user by the access network for addressing the user;
 - 10 - means for receiving (S-24) an internal IP address assigned by the service network (N-40) and included as an inner IP address within the tunnelled traffic to identify the user in the service network; and
 - 15 - means for linking said access credentials with the inner IP address and with the secure tunnel.
15. The user equipment (N-10; N-11) of claim 14, wherein the means for obtaining access credentials includes:
- means for receiving an authentication challenge from the core network;
 - 20 - means for generating and returning an authentication response to the core network;
 - means for generating a public and private key pair; and
 - 25 - means for submitting the public key along with a digital signature proving the ownership of the private key towards the core network.

16. The user equipment (N-10; N-11) of claim 14, wherein the means for obtaining access credentials includes:

REPLACEMENT SHEET

25

- means for receiving an authentication challenge from the core network;
- means for generating and returning an authentication response to the core network; and
- 5 - means for requesting a digital certificate obtainable from the core network.

10 17. The user equipment (N-10; N-11) of claim 16, wherein the means for obtaining access credentials further includes means for generating a public key for which the digital certificate is obtainable.

15 18. A method for supporting Single Sign-On services in a telecommunication service network (N-40) for a user (N-10) accessing said service network (N-40) through an access network (N-20) unable to provide data origin authentication, the user (N-10) having received (S-23) access credentials as a result of being authenticated by a core network (N-30), the method comprising the steps of:

- 20 - receiving (S-24) at the service network (N-40) the access credentials from the user (N-10) through the access network (N-20);
- checking (N-41, S-25, N-31) validity of the access credentials received at the service network (N-40);
- 25 - establishing (N-41, S-26, N-42) a valid session with the user (N-10) upon successful validity check of the access credentials;
- assigning at the service network (N-41, S-26, N-42) an internal IP address for the user (N-10) to identify

REPLACEMENT SHEET

26

the user when accessing a service in the service network; and

- 5 - linking (N-41, S-26, N-42) session data, access credentials and the assigned internal IP address for the user (N-10) at an entity (N-41; N-42) of the service network (N-40);

and characterised by including the steps of:

- 10 - establishing a secure tunnel (S-24) between the user equipment side (N-10) and an entity (N-41) of the service network (N-40) through the access network (N-20) by using an outer IP address assigned by the access network for addressing the user, and by using as an inner IP address in the tunnelled traffic the internal IP address assigned to identify the user in the service network (N-40); and
- 15

- linking said access credentials with said inner IP address and with said secure tunnel at the user equipment side (N-10).

- 20 19. The method of claim 18, further comprising a step of generating service credentials (N-41, S-26, N-42) for authorizing the user to access a service in the service network (N-40).

- 25 20. The method of claim 19, wherein the step of generating service credentials includes a step of generating service credentials on a per service basis for the user upon service request.

- 30 21. The method of claim 18, wherein the step of checking (N-41; N-41, S-25, N-31) the validity of access credentials received from the user (N-10) at the service network (N-40) further includes a step of communicating (S-25) with an Authentication Server (N-31) of the home network (N-

REPLACEMENT SHEET

27

30), when said access credentials are not signed by a recognised authentication entity.

5 22. The method of claim 18, wherein the step of linking session data, access credentials and assigned internal IP address for the user (N-10) further includes a step of communicating (S-26) a first device named Secure Service Entry Point (N-41), in charge of the secure tunnel (S-24), with a second device named Single Sign On Server (N-42) where the step of linking takes places.

10 23. The method of claim 18, for use when the user (N-10) is accessing a local service (N-44; N-45), or an external service (N-51) in a network (N-50) different than the currently accessed service network (N-40), the method further comprising a step of checking (S-28, N-42; S-32, N-42) whether the user had been previously authenticated
15 or not.